



DISEÑO DE UNA PLATAFORMA DE GESTIÓN Y MONITORIZACIÓN DE EVENTOS DE SEGURIDAD

Alejandro David Galera Ruiz

*Ingeniería de
Telecomunicación*



*Escuela Superior
de Ingenieros de Sevilla*



A mi familia, y en especial a mis padres, por todo su apoyo y esfuerzo que me han dedicado en mi época universitaria; a ellos les debo lo que soy, a dónde he llegado y lo que llegaré a ser.

A Mari Carmen, por ser un pilar tan importante en mi vida, por estar conmigo en los buenos y malos momentos, y por haberme llenado de alegría en todos estos años.

A mis amigos Carlos, Diego, Pablo, Enrique, Andrés, Diego N,... y un larguísimo etc, con los que he compartido años de convivencia e inolvidables momentos que han forjado una gran amistad.

A mis compañeros de Eneo Tecnología Pablo, Juan Jesús, Jaime, Alessandro... por haberme enriquecido enormemente con sus conocimientos y haberme hecho partícipe de un grupo de trabajo tan productivo e innovador.

A todos los que escapan de estas líneas pero no de mi mente y han puesto su granito de arena para que este proyecto sea posible, muchas gracias.

Autor: Alejandro David Galera Ruiz.

Tutor del Proyecto: D. Pablo Nebrera Herrera.

Área de Ingeniería Telemática

Departamento de Ingeniería de Sistemas y Automática

Escuela Superior de Ingenieros de la Universidad de Sevilla.

Julio 2006

ÍNDICE DE LA MEMORIA

1.INTRODUCCIÓN.....	6
1.1.Fases del proyecto.....	6
2.ESTRUCTURA GENERAL.....	7
2.1.Esquema estructural.....	7
3.DRAFT IDMEF. NORMALIZACIÓN DE LOGS DE SEGURIDAD.	9
3.1.Introducción.....	9
3.2.Modelo IDMEF. Generalidades.....	9
3.2.1.Problemas del modelo de datos solucionados con IDMEF.....	9
3.2.2.Razonamiento para implementar IDMEF en XML.....	10
3.3. El modelo de datos IDMEF y la DTD de XML.....	10
3.3.1.Perspectiva general del modelo de datos.....	11
3.3.2.Clase IDMEF-Message.....	12
4.ESTUDIO DE LAS SOLUCIONES PARA EL MOTOR DEL SISTEMA DE GESTIÓN DE MENSAJES.....	46
4.1.Estudio de Foresight.....	46
4.1.1.Introducción a Foresight.....	46
4.1.2.Clientes de evaluación Pasiva/activa.....	47
4.1.3.Clientes de sesión y datos de paquetes.....	47
4.1.4.Clientes de eventos Syslog y Procchck().....	48
4.1.5.Otros clientes.....	48
4.1.6.Prophet Server.....	48
4.1.7.Tablas de ejecución periódica (Crontab) para la interfaz Web.....	49
4.1.8.Desarrollo actual y tendencia.....	49
4.2.Estudio de Prelude.....	50
4.2.1.Introducción.....	50
4.2.2.Librería Libprelude.....	51
4.2.3.Librería Libpreludedb y la Base de Datos de Alertas.	51
4.2.4.Prelude-Manager.....	53
4.2.5.Prelude-LML.....	54
4.2.6.Sensores.....	54
4.3.Comparativa Prelude - Foresight.....	55
4.3.1.Salida cifrada SSL en XML.....	55
4.3.2.Base de datos escalable.....	55
4.3.3.Colector escalable.....	55
4.3.4.Compatibilidad con resto de sensores.....	55
4.3.5.Documentación.....	55
5.PRELUDE-IDS.....	56
5.1.Introducción.....	56
5.2.Instalación de Prelude.....	56
5.2.1.Instalación de los paquetes en Gentoo Linux.....	56
5.2.2.Instalación en resto de Linux.....	57
5.2.3.Configuración del Gestor de Prelude (Prelude-Manager).....	59
5.2.4.Creación de la base de datos de Prelude con PostgreSQL.....	60
5.2.5.Conexión de prelude-manager a la base de datos de eventos.....	63
5.2.6.Errores comunes.....	64
5.2.7.Actualización rc-update y esquema general del colector.....	65

6.SENSORES.....	66
6.1.Instalación de los Sensores.....	66
6.1.1.Registro de Prelude-LML.....	66
6.1.2.Configuración, ejecución y testeo de Prelude-LML.....	68
6.1.3.Errores comunes al arrancar Prelude-LML:.....	69
6.2.Snort IDS.....	71
6.2.1.Registro y conexión de Snort a Prelude-Manager.....	71
6.2.2.Errores Comunes.....	72
7.TESTEO DE PRELUDE.....	73
7.1.Testeo del conexiones.....	73
7.2.Testeo del envío de mensajes del cortafuegos Shorewall al Prelude-Manager.....	74
7.2.1.Carga de módulos para configuración de Shorewall.....	74
7.2.2.Configuración de ficheros de Shorewall.....	75
7.2.3.Comprobación de los mensajes en la base de datos.....	75
7.3.Testeo del sistema Prelude con Prewikka.....	76
7.4.Creación de un host virtual para Apache.....	77
7.5. Creación de un Alias Apache Prewikka sin host virtual.....	77
7.6.Capturas del testeo.....	78
8.DISEÑO EN JAVA DE LA LIBRERÍA PARA EL ACCESO Y MONITORIZACIÓN DE LA BASE DE DATOS: MARTEALERT.....	81
8.1.Introducción.....	81
8.2.JDBC.....	82
8.2.1.Uso del driver PostgreSQL JDBC.....	82
8.2.2.Instalación.....	83
8.3.Estructura de clases.....	84
8.4.Paquete common.....	85
8.4.1.Clase jTable.....	85
8.4.2.Clase jDatePicker.....	86
8.4.3.Clases gráficas.....	86
8.5.Paquete martealert.....	87
8.5.1.Clase martealertTable.....	87
8.5.2.Clase martealertTopStats.....	88
8.5.3.Clase martealertFirstLevel.....	99
8.5.4.Clase martealertRealTime.....	101
8.5.5.Clase martealertDetailedReport.....	103
8.5.6.Clase martealertAlertAgents.....	106
8.6.Paquete martealertFilter.....	107
8.6.1.Clase martealertHashtable.....	107
8.6.2.Clase martealertHashFilter.....	108
8.6.3.Clase martealertAdvancedFilterView.....	110
8.7.Paquete martealertUtils.....	112
8.7.1.Clase martealertCalendar.....	112
8.7.2.Clase martealertUtils.....	113
8.7.3.Clase martealertGlobals.....	114
8.7.4.Clase martealertSqlUtils.....	115

9.DESARROLLO EN POSTGRESQL.....	117
9.1.Gestión de la Base de datos con PGAdmin 3.....	117
9.1.1.Consulta de datos.....	118
9.1.2.Propiedades de la tabla. Restricciones y claves.....	119
9.2.Evolución de la estructura de las sentencias SQL.....	119
9.2.1.Salida de depuración de Prewikka.....	119
9.2.2.Optimización del tiempo de búsqueda.....	121
9.3.Comandos SQL.....	122
9.3.1.Método getCommand.....	122
9.4.Reindexado de libpreludedb.....	125
10.PRESUPUESTO.....	126
11.BIBLIOGRAFÍA.....	127
12.ANEXO 1: DIAGRAMA UML DE IDMEF.....	128
13.GLOSARIO.....	129